# 计算机网络安全

梅 挺/ 著

科学出版社

# 计算机网络安全

梅 挺 著

科学出版社

北京

## 内 容 简 介

本书是在广泛调研和充分论证的基础上，结合当前应用最为广泛的操作平台和网络安全规范写作而成，强调理论与实践相结合，具有科学、严谨的体系结构。全书内容丰富、构思新颖，全面阐述了网络安全理论与实践技术。

本书可作为网络安全领域的科技人员与信息系统安全管理人员的参考用书，也可作为高等院校研究生的教学用书。

**图书在版编目（CIP）数据**

计算机网络安全 / 梅挺著. —北京：科学出版社，2010
ISBN 978-7-03-029681-8

Ⅰ. ①计… Ⅱ. ①梅… Ⅲ. ①计算机网络-安全技术
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 237710 号

责任编辑：杨 岭 冯 铂 封面设计：陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

四川煤田地质制图印刷厂印刷
科学出版社发行 各地新华书店经销
*
2011 年 1 月第 一 版 开本：787×1092 1/16
2011 年 1 月第一次印刷 印张：20.25
印数：1—1500 字数：350 千字

**定价：60.00 元**

# 前　言

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。当前，网络安全问题在世界各国已经引起了普遍关注，已成为当今网络技术的一个重要研究课题。

在人类进入信息化时代的今天，人们对信息的安全传输、安全存储、安全处理的要求越来越高。信息安全不仅关系到战争的胜负、国家的安危、科技的进步和经济的发展，而且也关系到每个人的切身利益。我们看到，网络在加速人类社会信息化的同时，也给信息安全保障带来了极大的挑战。近几年来，网络犯罪呈逐年上升趋势。特别，随着电子商务、电子现金、数字货币、网络银行等业务的兴起以及各种专用网（如金融网）的建设，伴随着这些业务产生的互联网和网络信息的安全问题，也已成为人们关注的热点问题。

当前，我国的网络安全正面临着严峻的挑战：一方面随着电子政务工程的启动，电子商务的开展以及国家关键基础设施的网络化，使得现有的网络安全设施建设显得日益落后；另一方面，黑客入侵、病毒传播以及形形色色的网络攻击事件日益增多和成功率一直居高不下，从侧面反映出广大网民的网络防护意识和网络安全知识的欠缺。针对这种现状，作者在总结多年的实践经验和长期从事网络安全研究的基础上编写了本书。

本书是以 PDRR 模型为基础进行撰写的。在 PDRR 网络安全模型中，网络安全体系结构分成四部分：防护（Protection）、检测（Detection）、响应（Response）和恢复（Recovery）。从这个模型看，网络安全的建设是这样一个有机的过程：在信息安全管理政策的指导下，通过风险评估，明确需要防护的信息、网络基础设施和资产，然后利用入侵检测系统来发现外界的攻击和入侵，对已经发生的入侵，进行应急响应和恢复。PDRR 模型可以明确网络安全的每个组件在实际架构当中的角色和定位，有利于作为指南寻找未来研究和应用中的突破点。在安全防护部分重点介绍系统安全防护、网络安全防护和信息安全

防护。系统安全防护指的是操作系统的安全防护；网络安全防护中重点介绍网络安全管理政策、网络安全风险评估以及网络设备的访问权限控制；而信息安全防护则介绍信息安全当中的一些重要概念和内容。检测部分的主要内容是入侵检测系统的理论，包括入侵检测系统的概念、技术和评估以及入侵检测系统的发展前景。在响应和恢复部分中，重点介绍计算机紧急响应小组的建立及其业务；对于一个规模较大的网络来说，这样的一个组织的存在和运作是非常重要的。

本书是在广泛调研和充分论证的基础上，结合当前应用最为广泛的操作平台和网络安全规范，强调理论与实践相结合，具有科学严谨的体系结构，全书内容丰富、构思新颖，全面阐述了网络安全理论与实践技术。主要内容包括认证技术、数据安全技术、软件安全技术、Web 安全技术、网络互联安全技术、系统漏洞修复与扫描技术、虚拟网络应用技术、文件加密和数字签名技术、PKI 技术、系统灾难恢复技术、企业服务器安全配置技术等诸多重要技术。

本书得到了成都医学院学术著作出版基金资助，也是我主持的四川省教育厅资助项目“加密与纠错编码相结合——代数编码在现代密码学中的应用研究”的成果之一。本书得到了张仕斌教授的关心，并参阅了一些专家的研究成果。在此深表谢意。由于撰写时间仓促，书中疏漏之处在所难免，欢迎读者批评指正。

作　者

2010 年 11 月

# 目 录


**第 1 章 绪论** …… 1
1.1 网络安全基础知识 …… 1
1.1.1 计算机及网络所面临的安全威胁 …… 1
1.1.2 网络安全的基本概念 …… 4
1.1.3 网络安全体系结构 …… 6
1.1.4 常见的网络安全技术 …… 12
1.2 网络安全的规划与管理 …… 13
1.2.1 网络安全的规划与服务机制 …… 13
1.2.2 网络安全管理及规范 …… 14
1.3 网络安全策略与风险 …… 16
1.3.1 网络安全目标与策略 …… 16
1.3.2 网络安全风险与分析 …… 19
1.4 网络安全标准与法律法规 …… 21
1.4.1 网络安全标准 …… 21
1.4.2 网络安全法律法规 …… 23

**第 2 章 认证技术** …… 25
2.1 概述 …… 25
2.1.1 认证及认证模型 …… 25
2.1.2 认证协议 …… 26
2.2 口令认证技术 …… 28
2.2.1 安全口令 …… 28
2.2.2 静态口令认证技术 …… 30
2.2.3 动态口令认证技术 …… 30
2.3 消息认证技术 …… 33

2.3.1 采用 MAC 的消息认证技术 …… 33
2.3.2 采用 Hash 函数的消息认证技术 …… 36
2.4 实体认证技术 …… 39
2.4.1 身份认证系统 …… 39
2.4.2 通行字认证技术 …… 41
2.4.3 IC 卡认证技术 …… 42
2.4.4 个人特征识别技术 …… 47
2.4.5 Kerberos 身份认证技术 …… 48
2.5 X. 509 认证技术 …… 53
2.5.1 数字证书 …… 53
2.5.2 X. 509 认证过程 …… 54
2.5.3 PKI 技术 …… 55
2.5.4 PMI 技术 …… 63

**第 3 章 数据安全技术** …… 65
3.1 数据安全技术简介 …… 65
3.1.1 数据完整性 …… 65
3.1.2 数据备份 …… 67
3.1.3 数据压缩 …… 69
3.1.4 数据容错技术 …… 73
3.1.5 数据的保密与鉴别 …… 78
3.2 数据通信安全技术 …… 82
3.2.1 互联网模型应用保密和鉴别技术 …… 82
3.2.2 端对端保密和鉴别通信技术 …… 86
3.2.3 应用层上加数据保密和鉴别模块技术 …… 88

**第 4 章 软件安全技术** …… 90
4.1 概述 …… 90
4.1.1 软件安全的内涵 …… 90
4.1.2 软件安全面临的威胁 …… 92
4.2 软件安全 …… 93
4.2.1 软件加密技术 …… 93
4.2.2 防止非法复制技术 …… 93
4.2.3 防止软件跟踪技术 …… 97

4.2.4 法律/法规保护 …… 105
4.3 软件质量保证 …… 108
4.3.1 概述 …… 108
4.3.2 软件质量基本故障及分类 …… 109
4.3.3 软件质量控制和评估 …… 111
4.3.4 软件测试 …… 113

**第5章 Web安全技术** …… 115
5.1 概述 …… 115
5.2 Web的安全体系结构 …… 116
5.2.1 Web浏览器软件的安全需求 …… 117
5.2.2 主机系统的安全需求 …… 117
5.2.3 Web服务器的安全需求 …… 117
5.2.4 Web服务器上相关软件的安全需求 …… 118
5.3 Web安全协议 …… 119
5.3.1 SSL（安全套接层）协议 …… 119
5.3.2 TLS（传输层安全）协议 …… 125
5.3.3 SSL和TLS的区别 …… 126
5.3.4 IPSec协议 …… 128
5.4 Web服务器安全 …… 129
5.4.1 Web服务器的安全策略 …… 129
5.4.2 Web服务器的安全服务 …… 130
5.5 Web浏览器安全 …… 131
5.5.1 Web浏览器面临的威胁 …… 131
5.5.2 Web浏览器的安全策略 …… 133
5.5.3 Web浏览器的安全通信 …… 135

**第6章 网络互联安全技术** …… 138
6.1 概述 …… 138
6.1.1 网络互联的概念 …… 138
6.1.2 网络互联的实现方法 …… 139
6.2 局域网间的互联 …… 141
6.2.1 物理层间的互联 …… 141
6.2.2 链路层间的互联 …… 143

6.2.3 网络层间的互联 …… 143
6.2.4 应用层间的互联 …… 145
6.3 局域网与广域网间的互联 …… 146
6.3.1 概述 …… 146
6.3.2 局域网与广域网间互联的标准与交互操作性 …… 148
6.4 远程拨入局域网间的互联 …… 148
6.4.1 拨号接入技术 …… 148
6.4.2 ADSL 技术 …… 151
6.4.3 VPDN 技术 …… 151

**第 7 章 系统漏洞修复与扫描技术** …… 155
7.1 概述 …… 155
7.2 系统漏洞及防范 …… 156
7.2.1 IPC$ 默认共享漏洞 …… 156
7.2.2 Unicode 与二次解码漏洞 …… 157
7.2.3 IDQ 溢出漏洞 …… 158
7.2.4 Webdav 溢出漏洞 …… 159
7.2.5 SQL 空密码漏洞 …… 161
7.3 系统漏洞扫描与补丁更新技术 …… 162
7.3.1 利用系统本身及时更新系统补丁 …… 162
7.3.2 扫描并修复系统漏洞的工具软件简介 …… 164
7.4 基于 MBSA 的系统漏洞扫描与修复技术 …… 166
7.4.1 MBSA 简介 …… 166
7.4.2 MBSA 在系统漏洞扫描与修复的应用 …… 169

**第 8 章 虚拟网络应用技术** …… 171
8.1 虚拟专用网络（VPN）技术 …… 171
8.1.1 VPN 技术简介 …… 171
8.1.2 VPN 的关键安全技术 …… 174
8.1.3 VPN 的配置示例 …… 176
8.2 虚拟局域网（VLAN）技术 …… 185
8.2.1 VLAN 技术简介 …… 185
8.2.2 VLAN 配置示例 …… 187
8.3 专用虚拟局域网（PVLAN）技术 …… 196

8.3.1 PVLAN 技术简介 …… 196
8.3.2 PVLAN 的配置 …… 198

**第 9 章 文件加密和数字签名技术** …… 202
9.1 概述 …… 202
9.2 EFS 文件加密技术 …… 202
9.2.1 EFS 概述 …… 202
9.2.2 EFS 加密技术的应用 …… 203
9.3 加密数据的恢复 …… 204
9.3.1 数据恢复的基本思路 …… 204
9.3.2 配置 EFS 故障恢复代理模板 …… 205
9.3.3 申请 EFS 故障恢复代理证书 …… 207
9.3.4 添加域的故障恢复代理 …… 209
9.3.5 创建默认的独立计算机上的数据恢复代理 …… 211
9.4 密钥的存档与恢复 …… 213
9.4.1 密钥存档与恢复概述 …… 213
9.4.2 创建密钥恢复代理账户 …… 213
9.4.3 获取密钥恢复代理证书 …… 215
9.4.4 配置密钥存档与恢复属性 …… 215
9.4.5 创建新的可以进行密钥存档的证书模板 …… 217
9.4.6 获取具有存档密钥的用户证书 …… 218
9.4.7 执行密钥恢复示例 …… 220
9.4.8 导入已恢复的私钥 …… 222
9.5 PGP 动态文件加密和数字签名 …… 223
9.5.1 PGP 密钥的生成 …… 224
9.5.2 PGP 密钥的发布 …… 225
9.5.3 用 PGP 加密文件 …… 226
9.5.4 用 PGP 进行邮件数字签名 …… 228
9.6 电子签章 …… 230
9.6.1 iSignature 签章系统简介 …… 230
9.6.2 iSignature 主要功能 …… 231
9.6.3 个人数字证书申请 …… 231
9.6.4 iSignature 签章系统使用 …… 232
9.6.5 天威诚信安证通简介 …… 234

**第 10 章　PKI 技术** …… 238
10.1　PKI 概述 …… 238
10.2　证书基础 …… 238
10.2.1　证书服务概述 …… 238
10.2.2　证书服务的安装 …… 238
10.3　证书申请 …… 240
10.3.1　使用证书申请向导申请证书 …… 241
10.3.2　使用 Windows Server2003 证书服务网页 …… 245
10.4　证书的自动注册 …… 249
10.4.1　规划自动注册部署 …… 249
10.4.2　“用户”模板复制 …… 251
10.4.3　配置企业证书颁发机构 …… 252
10.4.4　建立自动注册域用户的策略 …… 253
10.5　证书的导入/导出 …… 254
10.5.1　概述 …… 254
10.5.2　导入证书 …… 255
10.5.3　导出证书 …… 256
10.5.4　导出带私钥的证书 …… 257
10.6　吊销证书和发布 CRL …… 257
10.6.1　吊销证书 …… 258
10.6.2　安排证书吊销列表（CRL）的发布 …… 260
10.6.3　手动发布证书吊销列表 …… 261
10.7　PKI 在文件传输加密与数字签名方面的应用 …… 262
10.7.1　配置密钥用法 …… 262
10.7.2　文件传输加密 …… 263
10.7.3　数字签名 …… 265
10.7.4　加密密钥对的获取 …… 266
10.7.5　邮件中的文件加密和数字签名 …… 268

**第 11 章　系统灾难恢复技术** …… 270
11.1　概述 …… 270
11.2　Active Directory 数据库备份与恢复技术 …… 271
11.2.1　备份 Active Directory 数据库 …… 271

11.2.2 还原 Active Directory 数据库 …… 273
11.3 SQL Server 2000 数据库备份与恢复技术 …… 276
11.3.1 数据库维护计划创建备份 …… 277
11.3.2 数据库的恢复 …… 280
11.4 操作系统灾难恢复技术 …… 282
11.4.1 Acronis True Image Server …… 282
11.4.2 Veritas 灾难恢复系统 …… 289

**第 12 章 企业服务器安全配置技术** …… 294
12.1 概述 …… 294
12.2 基于 Windows 系统的服务器安全配置 …… 294
12.2.1 系统安全加固 …… 294
12.2.2 基于 Windows 系统的 Web 服务器安全配置 …… 296
12.2.3 基于 Windows 系统的 FTP 服务器安全配置 …… 300
12.3 基于 Unix/Linux 系统的服务器安全配置 …… 301
12.3.1 基于 Unix/Linux 系统的 Web 服务器安全配置 …… 301
12.3.2 基于 Unix/Linux 系统的 FTP 服务器安全配置 …… 308

**参考文献** …… 312

# 第1章 绪 论

## 1.1 网络安全基础知识

伴随着科学技术的飞速发展，人们对 Internet 的依赖性越来越强，网络已经成为人们生活中不缺少的一部分。但是，互联网是一个开放、自由的系统，对信息系统的安全考虑并不完善。近年来，随着计算机和网络技术的广泛应用，计算机及其网络系统中被攻击与破坏事件不胜枚举。网络黑客犯罪已经渗入到各行各业，已成为现代社会的隐患，如果不加以保护，轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家的安全。目前，计算机及网络系统安全问题已经引起了世界各国的高度重视，他们不惜投入大量的人力、物力和财力来保障计算机及网络系统的安全性。

### 1.1.1 计算机及网络所面临的安全威胁

现在讲安全，已经不再像以前那样仅简单地谈计算机病毒，安全的防御也不再是仅安装了病毒软件和防火墙就能达到目的，这是因为计算机及网络系统所面临的威胁正随着计算机和网络技术的广泛应用在不段地增加。

**1. 计算机所面临的主要安全威胁**

随着个人计算机的普及，个人计算机也已成为黑客攻击的目标之一，就其计算机目前所面临的安全威胁而言，主要涉及以下几个方面。

(1) 计算机病毒

计算机病毒是当前计算机系统中最常见、最主要的威胁，几乎每天都有新的计算机病毒产生。计算机病毒有很多种，其主要危害体现在破坏计算机文件和数据，导致文件无法使用，系统无法启动；消耗计算机 CPU、内存和磁盘资源，导致一些正常服务无法进行，出现死机、占用大量的磁盘空间；有的还会破坏计算机硬件，导致计算机彻底瘫痪。

对于计算机病毒的防护，首先是安装计算机病毒防护软件（包括个人版或网络版），自动监测并查杀已感染的病毒。当然，对于高级用户来说也可以进行一些手工清除，但相对来说比较困难。

（2）木马

木马是一种基于远程控制的黑客工具，也称为“后门程序”。以前，我们一直说木马不是病毒，但是现在一些专家把木马也归属于病毒。但是木马和病毒确实存在许多本质上的区别。

目前，木马作为一种远程控制的黑客工具，主要危害包括窃取用户信息（比如计算机或网络帐户和密码、网络银行帐户和密码、QQ 帐户和密码、E-mail 帐户和密码等）；携带计算机病毒（造成计算机或网络不能正常运行，甚至完全瘫痪）；或被黑客控制，攻击用户计算机或网络。

（3）恶意软件

恶意软件是指一类特殊的程序，是介于计算机病毒与黑客软件之间的软件统称。它通常在用户不知晓也未授权的情况下潜入系统，具有用户不知道（一般也不许可）的特性，激活后将影响系统或应用的正常功能，甚至危害或破坏系统。其主要危害体现在非授权安装（也被称为“流氓软件”），自动拨号，自动弹出各种广告界面、恶意共享和浏览器窃持等。当前，恶意软件的出现、发展和变化给计算机系统和网络信息系统带来了巨大的危害。尽管已经出现了很多防范措施，但对恶意软件一般都很难防范，甚至无法删除。

**2. 网络所面临的主要安全威胁**

相对于个人计算机而言，网络所面临的安全威胁除具有计算机所面临的以上 3 种常见的威胁之外，还有就是网络黑客的入侵与攻击。由于互联网固有的缺陷，每个网络都有一定程度的漏洞和风险。黑客对网络的入侵和攻击有多种形式，可以是对网络系统直接或间接的攻击，例如非授权的泄露、篡改或删除等，在机密性、完整性或可用性等方面造成危害；也可能是偶发或蓄意的事件。

（1）系统漏洞威胁

系统漏洞是网络安全领域首要关注的问题，发现系统漏洞也是黑客进行入侵和攻击的主要步骤。据调查，国内 80%以上的网站存在明显的漏洞。漏洞的存在给网络上的不法分子的非法入侵提供了可乘之机，也给网络安全带来了巨大的风险。据美国 CERT/CC 统计，2006 年总共收到系统漏洞报告 8064 个，平均每天超过 22 个（自 1995 年以来，漏洞报告总数已经达到 30780 个）。这些漏洞的存在对广大互联网用户的系统造成了严重的威胁。

当前，操作系统的漏洞是我们面临的最大风险。比如，Windows 操作系统是目前使用最为广泛的系统，但经常发现存在漏洞。过去 Windows 操作系统的漏洞主要被黑客用来攻击网站，对普通用户没有多大影响，但近年来一些新出现的网络病毒利用 Windows 操作系统的漏洞进行攻击，能够自动运行、繁

衍、无休止地扫描网络和个人计算机，然后进行有目的的破坏。比如“红色代码”、“尼姆达”、“蠕虫王”，以及“冲击波”等。随着 Windows 操作系统越来越复杂和庞大，出现的漏洞也越来越多，利用 Windows 操作系统漏洞进行攻击造成的危害越来越大，甚至有可能给整个互联网带来不可估量的损害。

（2）人为因素的威胁

虽然人为因素和非人为因素都对计算机及网络系统构成威胁，但精心设计的人为攻击（因素）威胁最大。人为因素的威胁是指人为造成的威胁，包括偶发性和故意性威胁。具体来说主要包括网络攻击、蓄意入侵和计算机病毒等。一般来说，人为因素威胁可以分为人为失误和恶意攻击。

①人为失误。一是配置和使用中的失误，比如系统操作人员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不恰当，用户将自己的帐号随意转借给他人或信息共享等都会对网络安全带来威胁。二是管理中的失误，比如用户安全意识薄弱，对网络安全不重视，安全措施不落实，导致安全事故发生。据调查表明，在发生安全事件的原因中，居前两位的分别是“未修补软件安全漏洞”和“登录密码过于简单或未修改”，这表明了大多数用户缺乏基本的安全防范意识和防范常识。

②恶意攻击。恶意攻击是当前计算机及网络面临的最大威胁，主要分为两大类：一是主动攻击，它使用各种攻击方式有选择地破坏信息的完整性、有效性和可用性等；二是被动攻击，它是在不影响计算机及网络系统正常工作的情况下，进行信息的窃取、截获、破译等，以获取重要的机密信息。这两类攻击均能对计算机及网络系统造成极大的破坏，并导致机密信息泄露。

**3. 网络所面临的主要安全隐患**

隐患不等于威胁，但隐患来源于各种安全威胁。隐患所涉及的面要比威胁本身广得多，因为同一种威胁可能在不同方面造成安全隐患。

一般来说，个人网络安全问题仅限于与因特网连接时的网络安全，因此它唯一的安全隐患就是因特网。但对于企业网来说，其安全隐患不仅来自于因特网，内部网的安全隐患也非常值得重视，因为外网中的安全隐患同样也可以在内网中发生。即是说企业网的安全隐患有内、外网之分。正因为如此，企业网的安全策略设计中所考虑的不仅是病毒入侵、外网攻击那么简单了，而是要充分考虑内、外网的安全隐患，而且内、外网的安全隐患不是完全孤立的，在大多数情况下，对外网的安全问题最终来源于内网。

在当今开放式的网络环境中，网络安全隐患可以划分为以下几个大类：病毒、木马和恶意软件的入侵和感染；外部用户的攻击和入侵；内部网络用户的非法操作；数据备份与恢复等安全隐患。这些安全隐患主要表现为：

①由于黑客攻击所带来的机密信息泄露或网络服务器瘫痪。

②由于病毒、木马或恶意软件所带来的文件损坏或丢失，甚至计算机系统破坏。

③重要邮件或文件的非法访问、窃取或截获与操作等。

④关键部门未经授权的非法访问和敏感信息的泄露等。

⑤备份数据和存储媒介的损坏和丢失等。

针对以上的主要几类安全隐患，作为网络用户来说，采取的安全策略就是一定要安装专业的网络病毒防护系统（目前包括木马、恶意软件的检测和清除功能），加强内部网络的安全管理（因为木马、恶意软件也可以通过内部网络进行传播）；配置好防火墙过滤策略和系统本身的各项安全措施（如针对各类攻击所进行的通信协议安全配置），及时安装系统补丁（尽可能堵住系统本身所带来的安全隐患）；有条件的用户还可以在内、外网之间安装网络扫描检测、网络嗅探器（Sniffer）、入侵检测（IDS）和入侵防御（IPS）系统，甚至配置网络安全隔离系统，对内、外网进行安全隔离；加强内部网络的安全管理，严格执行“最小权限”原则，为各用户配置好恰当的用户权利和权限；同时对一些敏感数据进行加密保护，对发送的数据数据进行数字签名；根据网络系统的实际需要配置好相应的数据策略，并按策略认真执行。

### 1.1.2 网络安全的基本概念

计算机及网络所面临的安全威胁一直伴随着计算机和网络技术的发展而普遍存在着。从 20 世纪 70 年代开始，计算机及网络安全问题就日益突出；到 20 世纪 90 年代，网络安全已经威胁到了世界各国的利益，甚至威胁着世界各国的安全和主权问题，比如，1991 年巴格达军方的指挥系统遭到攻击、1994 年南非全民大选工作遭到干扰、1999 年 4 月国内大规模爆发 CIN 病毒（造成巨大损失）和 2001 年我国南部边境发生撞机事件等。由此可以看出，计算机及网络安全问题涉及到方方面面，包括技术上的问题、法律上的问题和社会问题等。

**1. 什么是网络安全**

一般意义上讲，安全就是指客观上不存在威胁，主观上不存在恐惧，或者说没有危险和不出事故，不受威胁。对计算机及网络系统来说，其安全问题也是如此，就是要保证整个计算机及网络系统的正确运行和不受威胁。网络安全既要保证网络系统物理硬件与设施的安全，又要保证软件系统与数据信息存储、传输和处理等全部过程的安全，即通常所说的保证网络系统运行的可靠性、信息的保密性、完整性和可用性等，而且还要保证网络服务不中断（连

续、可靠、安全地运行)。

由于现代的信息系统都是建立在网络基础之上的，因此网络安全也是信息系统的安全；而当今大家重点强调网络安全，是由于网络的广泛应用而使得安全问题变得尤为突出的缘故。因此，网络安全包括系统运行的安全、系统信息的安全保护、系统信息传播后的安全和系统信息内容的安全等四个方面的内容，即网络安全是对信息系统安全的运行、对运行在信息系统中的信息进行安全保护（包括信息的保密性、完整性和可用性保护等）、系统信息传播后的安全和系统信息内容的安全的统称。

①系统运行的安全是信息系统提供有效服务（即可用性）的前提，主要是保证信息处理和传输系统的安全，本质上是保护系统的合法操作和正常运行。主要涉及计算机系统机房环境的保护，法律、政策的保护，计算机结构设计的可靠安全运行，计算机操作系统和应用软件的安全，电磁信息泄露的防护等，它侧重于保证系统正常的运行，避免因系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免因电磁泄露，产生信息泄露，干扰他人(或受他人干扰)。

②系统信息的安全保护，主要是确保数据信息的保密性和完整性，包括用口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

③系统信息传播后的安全，包括信息过滤技术，它侧重于防止和控制非法、有害的信息进行传播后的后果，避免公用通信网络上大量自由传输的信息失控，本质上是维护道德、法律或国家利益。

④系统信息内容的安全，它侧重于网络信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等有损用户的行为，本质上是保护用户的利益和隐私。

**2. 网络安全的主要特征**

由前面内容可知网络安全主要涉及系统的可靠性、可用性和保密性等方面，因此网络系统的安全性也包括软件及数据的保密性、完整性、可用性和可靠性等。

①保密性（confidentiality)：主要是利用密码技术对软件和数据进行加密处理，保证在系统中存储和在网络上传输的软件和数据不被无关人员使用和识别。

②完整性（integrity)：是指保护网络系统中存储和传输的软件及数据不被非法操作，即保证数据不被插入、替换和删除，数据分组不丢失、乱序，数据库中的数据或系统中的程序或数据不被破坏等。